Eötvös Loránd Tudományegyetem
Természettudományi Kar

Mérai László

Pszeudovéletlen sorozatok és rácsok

című doktori értekezés tézisei

Matematikai Doktori Iskola
Vezető: Laczkovich Miklós

Elméleti Matematikai Doktori Program
Vezető: Szűcs András

Témavezető: Sárközy András

Budapest, 2010.

1. Bevezetés

Véletlen elemek generálása több alkalmazásban is központi szerepet játszik, különösen a kriptográfiában és a numerikus analízisben. Mivel valódi véletlen elemek sorozatának előállítása költséges, így a gyakorlatban nem valódi, hanem pszeudovéletlen értékeket használnak. A pszeudovéletlenségnek azonban több lehetséges definícióját is adták.

1997-ben Mauduit és Sárközy [11] a valódi véletlen sorozatok alapvető tulajdonságait alapul véve, egy új, kvantitatív követelményrendszert állított fel sorozatok véletlenségének vizsgálatához. Nevezetesen bevezették a véletlenség különböző mértékeit:

1. Definíció. *Adott* $E_N = \{e_1, \dots, e_N\} \in \{+1, -1\}^N$ *sorozat eloszlás mértéke:*

$$W(E_N) = \max_{a,b,t} |U(E_N, a, b, t)| = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|,$$

ahol a maximum olyan $a, b, t \in \mathbb{N}$ *számokra fut, melyekre* $1 \le a \le a + (t-1)b \le N$.

Az E_N *sorozat* ℓ*-ed rendű korrelációs mértéke:*

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right|,$$

ahol a maximum olyan $D = (d_1, \dots, d_\ell)$ ℓ*-eseken és* $M \in \mathbb{N}$ *számokon fut, melyekre* $d_1 < d_2 < \dots < d_\ell$, $M + d_\ell \le N$.

Ha E_N egy valódi véletlen sorozat, akkor mértékei kicsik ($W(E_N) \ll \sqrt{N \log N}$, illetve $C_\ell(E_N) \ll \sqrt{\ell N \log N}$, ld. [1]). Így egy E_N sorozatot jó pszeudovéletlen tulajdonságokkal rendelkező sorozatnak tekinthetünk, ha mértékeire $\log N$ hatványától eltekintve hasonló korlát adható, legalább kis ℓ korrelációs rendekre.

Goubin, Mauduit és Sárközy [4] a Legendre szimbólum segítségével definiált jó pszeudovéletlen sorozatot (kiterjesztve Mauduit és Sárközy [11] konstrukcióját):

1. Konstrukció (Goubin, Mauduit, Sárközy). *Legyen* p *egy prímszám,* $f \in \mathbb{F}_p[x]$ *és definiáljuk az* $E_p = \{e_1, \dots, e_p\}$ *sorozatot a következőképpen:*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right), & \text{ha } p \nmid f(n), \\ 1, & \text{ha } p \mid f(n), \end{cases}$$

ahol $\left(\frac{\cdot}{p}\right)$ *a Legendre szimbólum.*

Később Mauduit, Rivat és Sárközy [10] könnyen számolható konstrukciót vizsgált:

2. Konstrukció (Mauduit, Rivat, Sárközy). *Legyen p egy prímszám és $f \in \mathbb{F}_p[x]$. Definiáljuk az $E_p = \{e_1, \dots, e_p\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } f(n) \in \{1, 2, \dots, \frac{p-1}{2}\} \\ -1, & \text{máskülönben.} \end{cases}$$

Megmutatták, hogy a konstrukció csak erős megszorításokkal mondható pszeudovéletlennek. Nevezetesen, ha a polinom foka nagyobb, mint a korreláció rendje, akkor a korrelációs mérték lehet nagy. Ezt a hiányosságot küszöbölte ki Mauduit és Sárközy, lecserélve az f polinomot annak multiplikatív inverzével:

3. Konstrukció (Mauduit, Sárközy). *Legyen p egy prímszám és $f \in \mathbb{F}_p[x]$. Definiáljuk az $E_p = \{e_1, \dots, e_p\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } f(n) \neq 0 \text{ és } f(n)^{-1} \in \{1, 2, \dots, \frac{p-1}{2}\} \\ -1, & \text{máskülönben,} \end{cases}$$

ahol a^{-1} $(a \neq 0)$ az $a \in \mathbb{F}_p$ elem multiplikatív inverzét jelöli.

2. Pszeudovéletlen bináris sorozatok általános konstrukciója

Az eddig felsorolt konstrukciókat mind a következő általános konstrukció speciális eseteiként kapjuk:

4. Konstrukció. *Legyen p prímszám, ψ additív, χ multiplikatív karaktere $\mathbb{F}_p$-nek, $F(x)$, $Q(x) \in \mathbb{F}_p(x)$ racionális törtfüggvények. Ekkor definiáljuk az E_p sorozatot a következő módon:*

$$e_n = \begin{cases} +1 & \text{ha } \arg\left(\psi\left(F(n)\right) \cdot \chi\left(Q(n)\right)\right) \in [0, \pi) \text{ és } n \notin S \\ -1 & \text{máskülönben.} \end{cases}$$

Világos, hogy ha az F függvényt konstansnak és a χ karaktert a kvadratikus karakternek választjuk, akkor visszakapjuk az 1. konstrukciót. Másrészről, ha a χ karaktert úgy választjuk, hogy $\chi(g) = e^{\frac{2\pi i}{p-1}}$, ahol g generátor $\mathbb{F}_p$-ben akkor Gyarmati [5] és Sárközy [16] diszkrét logaritmus segítségével definiált konstrukcióját kapjuk.

Továbbá, ha a Q függvény konstans, akkor visszakapjuk a 2. illetve a 3. konstrukciót, amennyiben az F függvény egy polinom vagy annak multiplikatív inverze.

Pszeudovéletlen bináris sorozatok konstrukcióját ilyen általánosságban először Oon tanulmányozta [14, 15]. Vizsgálta a 4. konstrukció azon speciális esetét, mikor az F függvény konstans. Bebizonyította, hogy a konstrukció jó, ha a karakter rendje

nagy: $\Omega(p^{1/2})$. Abban az esetben, amikor a karakter rendje kicsi (nagyságrendileg $o(p^{1/2})$) és páratlan, akkor nem várhatunk nemtriviális korlátot (ld 3. fejezet 1. példa).

Először azt vizsgáltam, hogy lehet-e jó korlátot adni abban az esetben, mikor a karakter rendje kicsi (nagyságrendileg $o(p^{1/2})$) és páros.

A megfelelő tétel kimondása előtt definiálni kell a megengedhetőség fogalmát, amely karakterizálja, mely Q függévnyek esetén adható jó felső korlát a mértékekre.

2. Definíció. *A (k,ℓ,m) számhármas d-megengedhető $(k,\ell<m)$, ha nem létezik a következő követelményeknek eleget tevő $\mathcal{A},\mathcal{B}$ multihalmaz:*

(i) $|\mathcal{A}|=k$, $|\mathcal{B}|=\ell$;

(ii) *$\mathcal{A}$ és $\mathcal{B}$ minden elemének multiplicitása kisebb, mint d, és $\mathcal{A}$ minden elemének multiplicitása relatív prím d-hez;*

(iii) *az $\mathcal{A}+\mathcal{B}$ összegben minden elem d-szeresen van reprezentálva, azaz az*

$$a+b=c,\quad a\in\mathcal{A},b\in\mathcal{B}$$

egyenletnek a megoldásszáma minden c esetén osztható d-vel.

(Itt $|\mathcal{A}|$ az $\mathcal{A}$ multihalmaz különböző elemeinek a számát jelöli.)

Továbbá a (k,ℓ,G) hármas megengedhető, ha minden $\mathcal{A},\mathcal{B}\subset G$ halmaz esetén, melyre $|\mathcal{A}|\le k$, $|\mathcal{B}|\le\ell$ létezik olyan $c\in G$ elem, hogy az

$$a+b=c\quad a\in\mathcal{A},\ b\in\mathcal{B}$$

egyenletnek pontosan egy megoldása van.

3. Tétel ([M1]). *Ha az E_p sorozatot a 4. konstrukció definiálja, ahol a χ multiplikatív karakter d rendje páros, $Q\in\mathbb{F}_p[x]$ polinom, ami nem d-hatvány, és az F függvény konstans, akkor*

$$W(E_p)\le 36sp^{1/2}\log p\log d+s,$$

ahol s a Q gyökeinek számát jelöli.

Továbbá ha a Q minden gyökének multiplicitása vagy relatív prím d-hez, vagy azzal osztható, és az (s,ℓ,p) hármas d-megengedhető, akkor

$$C_\ell(E_p)\le 9\,4^\ell\ell sp^{1/2}\log p(\log d)^\ell+\ell s.$$

Ha az F függvény nem konstans, akkor a χ karakter rendje lehet páratlan is:

4. Tétel ([M3]). *Legyen $\psi\neq\psi_0$ additív, $\chi\neq\chi_0$ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek, $F(x)=\frac{f(x)}{g(x)},Q(x)=\frac{q(x)}{r(x)}\in\mathbb{F}_p(x)$ olyan racionális törtfüggvények, melyekre*

$(g(x), f(x)) = 1$, $(q(x), r(x)) = 1$ *és sem* f*-nek, sem* g*-nek nincs többszörös gyöke,* Q *pedig nem* d*-hatvány. Ha az* E_p *sorozatot a 4. konstrukció definiálja, akkor*

$$W(E_p) \ll (\deg^* F + z) \cdot p^{1/2} (\log p)^2,$$

ahol z *jelöli* q *és* r *különböző gyökeinek számát.*

Továbbá, ha $\ell \in \mathbb{N}$ *teljesíti az alábbi feltételek valamelyikét:*

(i) $\ell = 2$*;*

(ii) $(4 \cdot \deg g)^\ell < p$, $(4 \cdot \deg^* Q)^\ell < p$*;*

(iii) $g(x) = (x + a_1)(x + a_2) \dots (x + a_k)$ *(* $a_i \neq a_j$*,* $i \neq j$ *) és* $\ell \cdot \deg g < \frac{p}{2}$, $(4 \cdot \deg^* Q)^\ell < p$*,*

akkor

$$C_\ell(E_p) \ll (\ell + 1)(\deg^* F + d \cdot \deg^* Q) \cdot p^{1/2} (\log p)^{\ell+1}.$$

Hasonlóan bizonyítható az az eset is, mikor a Q függvény konstans [M2]. Ekkor a tételben szereplő korlátok megfelelői érvényesek.

3. Pszeudovéletlen bináris rácsok

Az alkalmazásokban a pszeudovéletlen sorozatok mellet komoly igény mutatkozott pszeudovéletlen rácsok iránt is. Ezért Hubert, Mauduit és Sárközy kiterjesztette a pszeudovéletlen bináris sorozatok fogalmát több dimenzióra [9]. Legyen I_N^n a következő halmaz:

$$I_N^n = \left\{ \mathbf{x} = (x_1, \dots, x_n) : \, x_1, \dots, x_n \in \{0, 1, \dots, N-1\} \right\}.$$

Ekkor a bináris rácsot mint az I_N^n halmazon értelmezett bináris függvényt definiáljuk:

$$\eta : I_N^n \to \{-1, +1\}.$$

Az egydimenziós esethez hasonlóan definiálhatjuk a mértékeket. Ehhez legyen először $\mathbf{u}_1, \dots, \mathbf{u}_n$ n darab lineárisan független vektor, melyeknek $n-1$ koordinátája nulla. Legyenek $t_1, \dots, t_n$ olyan egészek, melyekre $0 \leq t_1, \dots, t_n < N$. Ekkor B_N^n (vagy röviden B) *tégla rácsot* (box lattice) a következőképpen definiáljuk:

$$B_N^n = \left\{ \mathbf{x} = x_1\mathbf{u}_1 + \dots + x_n\mathbf{u}_n : \, 0 \leq x_i |\mathbf{u}_i| \leq t_i, \; i = 1, \dots, n \right\}.$$

5. Definíció. *Az* η *sorozat* ℓ*-ed rendű véletlenségi mértéke a*

$$Q_\ell(\eta) = \max_{B, \mathbf{d}_1, \dots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d}_1) \dots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|,$$

ahol a maximum az összes $\mathbf{d}_1, \dots, \mathbf{d}_\ell \in I_N^n$ *és* B *téglarácsra fut, melyre* $B + \mathbf{d}_1, \dots, B + \mathbf{d}_\ell \subseteq I_N^n$.

Huber, Mauduit és Sárközy szintén vizsgálta, hogy hogyan viselkednek ezen mértékek valódi véletlen esetben. Bebizonyították, hogy ha $\eta : I_N^n \to \{-1, +1\}$ egy valódi véletlen rács, akkor $Q_\ell(\eta) \ll \sqrt{\ell\, N^n \log N^n}$ (ld. [9]). Ezek alapján egy η rácsot jó pszeudovéletlen tulajdonságokkal rendelkező rácsnak tekinthetünk, ha mértékeire nagyságrendileg hasonló korlát adható, legalább kis ℓ rendekre.

Mauduit és Sárközy [13] példát mutatott jó pszeudovéletlen rácsra:

5. Konstrukció (Mauduit és Sárközy). *Legyen $q = p^n$ prímhatvány, γ a kvadratikus karaktere $\mathbb{F}_q$-nak, $f(x) \in \mathbb{F}_q[x]$. Ekkor definiáljuk az η rácsot a következőképpen:*

$$\eta(\mathbf{x}) = \begin{cases} \gamma(f(x_1 b_1 + \cdots + x_n b_n)) & \text{ha } f(x_1 b_1 + \cdots + x_n b_n) \neq 0, \\ 1 & \text{máskülönben,} \end{cases}$$

ahol $b_1, \ldots, b_n$ $\mathbb{F}_q$ egy bázisa $\mathbb{F}_p$ fölött és $\mathbf{x} = (x_1, \ldots, x_n)$.

Bebizonyították, hogy ha f kielégít bizonyos feltételeket, akkor ez a konstrukció jó:

$$Q_\ell(\eta) < \deg f\, \ell(q^{1/2}(1 + \log p)^n + 2).$$

Megjegyezem, hogy mind a bináris rács fogalmát, mind a mértékeket ki lehet terjeszteni több szimbólumú esetre, ld. [M5].

Az 5. konstrukciót a sorozatokhoz hasonlóan kiterjeszthetjük általános multiplikatív karakter segítségével:

6. Konstrukció. *Legyen $q = p^n$ prímhatvány, $f(x) \in \mathbb{F}_q[x]$, χ multiplikatív karaktere $\mathbb{F}_q$-nak. Ekkor definiáljuk az η rácsot a következőképpen:*

$$\eta(\mathbf{x}) = \begin{cases} +1 & \text{ha } \arg\left(\chi(f(x_1 b_1 + \cdots + x_n b_n))\right) \in [0, \pi), \\ -1 & \text{másülönben,} \end{cases}$$

ahol $b_1, \ldots, b_n$ $\mathbb{F}_q$ egy bázisa $\mathbb{F}_p$ fölött és $\mathbf{x} = (x_1, \ldots, x_n)$.

A következő tétel alapján ez egy jó konstrukció:

6. Tétel ([M4]). *Definiálja az η rácsot a 6. konstrukció. Legyen a χ multiplikatív karakter d rendje páros, $f(x) \in \mathbb{F}_q[x]$ olyan polinom mely nem d-hatvány, és minden gyökének multiplicitása vagy osztható d-vel, vagy ahhoz relatív prím. Tegyük fel továbbá, hogy a $(\deg f, \ell, \mathbb{F}_q)$ hármas megengedhető. Ekkor*

$$Q_\ell(\eta) \leq 4^\ell \ell \deg f (\log d)^\ell q^{1/2} (1 + \log p)^n \ell \deg f.$$

4. Pszeudovéletlen bináris sorozatok és rácsok elliptikus görbék felett

Kriptográfiai alkalmazásokban előszeretettel használnak elliptikus görbéket, azok véletlen viselkedése miatt. Elliptikus görbék segítségével először Hallgren definiált sorozatot a következő módon [8]: Adott $\mathcal{E}$ elliptikus görbe és $P, P_0 \in \mathcal{E}$ pont esetén legyen $s_0 = P_0$ és

$$s_n = P \oplus s_{n-1} = nP \oplus P_0.$$

Chen [2], illetve később Chen, Li, és Xiao [3] tanulmányozta az ebből a sorozatból származtatható bináris sorozatokat, ahol a bináris sorozatot a Legendre szimbólum, illetve véges testek fölötti diszkrét logaritmus segítségével származtatták.

Az általános konstrukciót a következőképp definiálhatjuk:

7. Konstrukció. *Legyen $p > 3$ prímszám, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ fölött, $G \in \mathcal{E}(\mathbb{F}_p)$ T-ed rendű elem, $f \in \mathbb{F}_p(\mathcal{E})$, χ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek. Ekkor definiáljuk az $E_T = \{e_1, \ldots, e_T\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } nG \notin \operatorname{Supp}(f) \text{ és } \arg\big(\chi(f(nG))\big) \in [0, \pi), \\ -1, & \text{máskülönben.} \end{cases}$$

Hasonlóan a korábbiakhoz, ha χ a Legendre szimbólum, akkor visszakapjuk Chen konstrukcióját [2]. Másrészről, ha χ $p-1$-ed rendű karakter, akkor megkapjuk Chen, Li és Xiao diszkrét logaritmuson alapuló konstrukcióját [3].

7. Tétel ([M7]). *Ha az $E_T = \{e_1, \ldots, e_T\}$ sorozatot a 7. konstrukció definiálja, ahol a χ karakter rendje páros, $f \in \mathbb{F}_p(\mathcal{E})$ nem d-hatvány $\overline{\mathbb{F}}_p(\mathcal{E})$-ben és G T-ed rendű pont, akkor*

$$W(E_T) \leq 4|\operatorname{Supp}(f)|p^{1/2}(1 + \log T)\log d + |\operatorname{Supp}(f)|.$$

Továbbá, ha f gyökeinek és pólusainak multiplicitása vagy d-vel osztható, vagy ahhoz relatív prím, $\ell \in \mathbb{N}$ olyan egész, melyre a $(|\operatorname{Supp}(f)|, \ell, T)$ hármas d-megengedhető, akkor

$$C_\ell(E_T) \leq 4^\ell |\operatorname{Supp}(f)|p^{1/2}(1 + \log T)(\log d)^\ell + \ell|\operatorname{Supp}(f)|.$$

További jó konstrukciót definiálhatunk racionáls törtfüggvény maradékával is:

8. Konstrukció. *Legyen $p > 3$ prímszám, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ fölött, $G \in \mathcal{E}(\mathbb{F}_p)$ T-ed rendű elem, $f \in \mathbb{F}_p(\mathcal{E})$. Ekkor definiáljuk az $E_T = \{e_1, \ldots, e_T\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } f(nG) \in \{0, 1, \ldots, \frac{p-1}{2}\}, \\ -1, & \text{máskülönben.} \end{cases}$$

8. Tétel ([M8]). *Legyen $p > 3$ prímszám, $f \in \mathbb{F}_p(\mathcal{E})$ nem konstans függvény. Ha az $E_T = \{e_1, \dots, e_T\}$ sorozatot a 8. konstrukció definiálja, akkor*

$$W(E_T) << \deg f \, p^{1/2} \log p \log T.$$

Ha feltesszük továbbá, hogy
(i) $\deg f < p(T)$ *és* $\ell = 2$;
(ii) $\deg f < p(T)$ *és* $(4 \deg f)^\ell < p(T)$,
ahol $p(T)$ a T legkisebb prímosztója, akkor

$$C_\ell(E_T) << \ell \deg f p^{1/2} (\log p)^\ell \log T.$$

Végül megmutatom, hogy elliptikus görbék segítségével jó pszeudovéletlen rács is definiálható.

9. Konstrukció. *Legyen $p > 3$ prímszám, χ multiplikatív karaktere $\mathbb{F}_p$-nek, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ fölött, $f \in \mathbb{F}_p(\mathcal{E})$ és $P_1, \dots, P_n \in \mathcal{E}(\mathbb{F}_p)$ olyan gyengén független pontok, melyek rendje nem nagyobb N-nél. Ekkor definiáljuk az $\eta : I_N^n \to \{-1, +1\}$ rácsot a következő módon:*

$$\eta(x_1, \dots, x_n) = \begin{cases} +1 & \text{ha } x_1 P_1 \oplus \dots \oplus x_n P_n \notin \operatorname{Supp}(f) \\ & \quad \text{és } \arg\big(\chi(f(x_1 P_1 \oplus \dots \oplus x_n P_n))\big) \in [0, \pi), \\ -1 & \text{másképpen.} \end{cases}$$

9. Tétel ([M6]). *Legyen $p > 3$ prímszám, χ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek, melynek rendje páros. Legyen továbbá $f \in \mathbb{F}_p(\mathcal{E})$, mely nem d-hatvány $\overline{\mathbb{F}}_p(\mathcal{E})$-ben, és az f gyökeinek és pólusainak rendje vagy osztható d-vel, vagy d-hez relatív prím. Ha az $\eta : I_N^n \to \{-1, +1\}$ rácsot a 9. konstrukció definiálja, és a $(|\operatorname{Supp}(f)|, \ell, \mathcal{E}(\mathbb{F}_p))$ hármas megengedhető, akkor*

$$Q_\ell(\eta) \le 2 \cdot 3^n (2d)^\ell \ell d \deg(f) p^{1/2} (\log |\mathcal{E}(\mathbb{F}_p)|)^n (\log d)^\ell + \ell |\operatorname{Supp}(f)|.$$

5. Megengedhetőség

A következőkben elégséges feltételeket adok d-megengedhetőségre, illetve megengedhetőségre.

10. Tétel ([M7]). *Egy m szám legkisebb prímosztóját jelölje $p(m)$. Ekkor*
(i) Ha $k, m, d \in \mathbb{N}$, $k < p(m)$, akkor a $(k, 2, m)$ hármas d-megengedhető.
(ii) Ha $k, m, d \in \mathbb{N}$, $k < p(m)$, továbbá $(4\ell)^k < p(m)$, akkor a (k, ℓ, m) hármas d-megengedhető.

(iii) Ha m egy prímszám, d minden prímosztója primitív gyök modulo m, akkor minden $k, \ell < m$ esetén a (k, ℓ, m) hármas d-megengedhető.

11. Tétel ([M6]). *Legyen $G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}$ tetszőleges véges Abel csoport, és $p(G)$ a csoport rendjének legkisebb prímosztója. Legyen $k, \ell \in \mathbb{N}$ melyek az alábbi feltételek valamelyikét teljesítik:*

(i) $k < p(G)$, $\ell = 2$;

(ii) $4^{s(k+\ell)} < p(G)$.

Ekkor a (k, ℓ, G) hármas megengedhető.

Az értekezés a szerző alábbi cikkeit dolgozza fel

[M1] L. Mérai, Construction of large families of pseudorandom binary sequences, The Ramanujan Journal 18 (2009), 341–349.

[M2] L. Mérai, A construction of pseudorandom binary sequences using rational functions, Unif. Distrib. Theory, 4 (2009), no. 1, 35–49.

[M3] L. Mérai, A construction of pseudorandom binary sequences using both additive and multiplicative characters, Acta Arith. 139 (2009), 241–252.

[M4] L. Mérai, Construction of pseudorandom binary lattices based on multiplicative characters, Periodica Math. Hungar. 59 (2009) 43–51.

[M5] L. Mérai, On finite pseudorandom lattices of k symbols, Monatsh. Math. 161 (2010), no. 2, 173–191.

[M6] L. Mérai, Construction of pseudorandom binary lattices using elliptic curves, Proc. Amer. Math. Soc. 139 (2011), 407-420

[M7] L. Mérai, Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters, beküldve

[M8] L. Mérai, Construction of pseudorandom binary sequences over elliptic curves, beküldve

További hivatkozások

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, Measures of pseudorandomness for finite sequences: typical values, Proc. Lond. Math. Soc. (3) 95 (2007) no. 3, 778–812.

[2] Z. Chen, Elliptic curve analogue of Legendre sequences, Monatsh. Math. 154 (2008) no. 1, 1–10.

[3] Z. Chen, S. Li, G. Xiao, G. Construction of pseudorandom binary sequences from elliptic curves by using discrete logarithm, Lecture Notes in Comput. Sci., 4086, Springer, Berlin, (2006) 285-294.

[4] L. Goubin, C. Mauduit, and A. Sárközy, Construction of large families of pseudorandom binary sequences, J. Number Theory 106 (2004), 56–69.

[5] K. Gyarmati, On a family of pseudorandom binary sequences, Periodica Math. Hungar. 49 (2004) 45-63.

[6] K. Gyarmati; C. Mauduit; A. Sárközy: Constructions of pseudorandom binary lattices. Unif. Distrib. Theory 4 (2009), no. 2, 59–80.

[7] K. Gyarmati; A. Sárközy; C. L. Stewart: On Legendre symbol lattices. Unif. Distrib. Theory 4 (2009), no. 1, 81–95.

[8] S. Hallgren, Linear congruential generators over elliptic curves, Tech. Report CS-94-143, Carnegie Mellon Unv., 1994.

[9] P. Hubert, C. Mauduit and A. Sárközy, On pseudorandom binary lattices, *Acta Arith.* **125** (2006), 51–62.

[10] C. Mauduit, J. Rivat and A. Sárközy, *Construction of pseudorandom binary sequence using additive characters*, Monatshefte Math. 141 (2004), 197–208

[11] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol, Acta Arith. 82 (1997), 365–377.

[12] C. Mauduit, A. Sárközy, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239–252.

[13] C. Mauduit, A. Sárközy, On large families of pseudorandom binary lattices, *Unif. Distrib. Theory* **2** (2007), no. 1, 23–37.

[14] S. M. Oon, *Construction des suites binaires pseudo-aléatories*, PhD dolgozat, Nancy, 2005.

[15] S. M. Oon, *On pseudo-random properties of certain Dirichlet series*, Ramanujan J. 15 (2008), no. 1, 19–30

[16] A. Sárközy, A finite pseudorandom binary sequence, Studia Sci. Math. Hungar. 38 (2001), 377-384.